PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
LAWRENCE ROSENTHAL
STROOCK & STROOCK & LAVAN LLP
180 MAIDEN LANE
NEW YORK, NY 10038

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*) 27 AUG 2004

Applicant's or agent's file reference
097229/0047

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/10507	05 April 2004 (05.04.2004)	07 April 2003 (07.04.2003)

International Patent Classification (IPC) or both national classification and IPC
IPC(7): G06F 12/14 and US Cl.: 713/201

Applicant
ITRACS CORPORATION

1. This opinion contains indications relating to the following items:

☒ Box No. I Basis of the opinion

□ Box No. II Priority

□ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

□ Box No. IV Lack of unity of invention

☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

□ Box No. VI Certain documents cited

☒ Box No. VII Certain defects in the international application

☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer Michelle R.
for
Justin T. Darrow

Telephone No. (703) 305-3900

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US04/10507

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   □ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      □ a sequence listing

      □ table(s) related to the sequence listing

   b. format of material

      □ in written format

      □ in computer readable form

   c. time of filing/furnishing

      □ contained in international application as filed.

      □ filed together with the international application in computer readable form.

      □ furnished subsequently to this Authority for the purposes of search.

3. □ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/10507

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	9, 10, 15, 16, and 18-20	YES
	Claims	1-8, 11-14, 17, 21, and 22	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-22	NO
Industrial applicability (IA)	Claims	1-22	YES
	Claims	NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The drawings are objected to under PCT Rule 66.2(a)(iii) as containing the following defect(s) in the form or content thereof: Figure 1 is objected to because it fails to show the local area network, the security server, and the administration terminal of items 150, 152, and 154, respectively as described in the description (see page 5, ¶ [0017]). Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing.

Claim 11 is objected to under PCT Rule 66.2(a)(iii) as containing the following defect in the form or contents thereof: Claim 11 is objected as being of improper dependent form for failing to further limit the subject matter of a claim 1.

Claim13 is objected to under PCT Rule 66.2(a)(iii) as containing the following defect in the form or contents thereof: after "plurality" in line 1, insert --of--.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.	PCT/US04/10507

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

Claims 1-11 are objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claims 1-11 are indefinite for the following reason: Claim 1 is incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. The omitted structural cooperative relationships are: the workstation coupled via a computer network.

Claim 10 is objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claim 10 is indefinite for the following reason: Claim 10 recites the limitation "said event log" in line 1. There is insufficient antecedent basis for this limitation in the claim.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US04/10507	

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

Claims 1-8, 11-14, 17, 21, and 22 lack novelty under PCT Article 33(2) as being anticipated by Ensor et al., U.S. Patent No. 5,721,780 A.

As per claims 1 and 21, Ensor et al. illustrate a method and computer readable medium for providing security to a computer network by monitoring the physical location of a network login or login attempt, comprising:

associating a workstation to a physical location (see column 4, lines 19-25; figure 1, items 110 and 112; a terminal device for a home subscriber station connected by a telephone jack and line);

associating a network user to the workstation (see column 3, lines 62-67; a user who has a particular subscriber terminal);

monitoring a computer network to determine a network login or attempted login of the user (see column 4, lines 40-59; receiving from the network a unique, network coupling identifier for the particular terminal when the subscriber attempts to gain access to the network);

determining a physical location of the login or attempted login (see column 4, lines 51-63; figure 1, item 112 and 122; determining the location of the terminal from the unique, network coupling identifier associated with the dedicated telephone line coupling the terminal to the network); and

determining whether the user is authorized to access the network from the physical location of the login or attempted login (see column 5, lines 54-67; column 6, lines 1-6; figure 1, items 110, 112, 126, and 114; the transaction manager compares the newly encrypted password with the retrieved password where two nonidentical passwords indicate an unauthorized login attempt and two identical passwords indicate successful authentication for the subscriber to access the network at the dedicated telephone line).

As per claim 2, Ensor et al. then point out:

determining whether preventative action is necessary (see column 5, lines 58-60; figure 1, item 114; comparing if the newly encrypted password is identical to the retrieved password), and

if so (see column 5, lines 60-61; if the two passwords are not identical), automatically initiating preventative action (see column 5, lines 60-66; figures 110, 112, and 126; sending an error message to the subscriber that the authentication has failed).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/10507

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

As per claim 3, Ensor et al. further describe:

generating an alert (see column 5, lines 60-66; figures 110, 112, and 126; sending an error message to the subscriber that the authentication has failed).

As per claim 4, Ensor et al. additionally mention:

disconnecting the workstation from the network (see column 6, line 1; the modem connection is terminated).

As per claim 5, Ensor et al. then discuss:

generating a notification message that the user is accessing the computer network from an unauthorized location (see column 5, lines 60-66; an error message is sent indicating a mismatch between the particular terminal and the dedicated telephone line at an unauthorized location for the subscriber).

As per claim 6, Ensor et al. moreover elaborate:

storing information regarding the physical location of the login (see column 6, lines 26-42; figure 1, items 108, 112, and 110; updating the password for the subscriber by encrypting the network coupling identifier with a different encryption key) and the attempted login (see column 5, lines 22-27; creating a subscriber registration account by the newly encrypted password representative of the telephone number of the particular terminal).

As per claim 7, Ensor et al. next describe:

storing information regarding the workstation associated with the login (see column 6, lines 26-42; figure 1, item 110, 108, and 112; updating the corresponding list of passwords by encrypting the network coupling identifier using a different encryption key after an initial password authentication for a selected terminal) and attempted login (see column 5, lines 22-27; registering the particular terminal attempting to login by creating a subscriber registration account in the database identified by the newly encrypted password).

As per claim 8, Ensor et al. also specify:

workstation information including the jack or outlet information (see column 6, lines 26-42; figure 1, item 110, 108, and 112; updating the corresponding list of passwords by encrypting the network coupling identifier using a different encryption key after an initial password authentication for a selected terminal; see column 4, lines 51-63; figure 1, item 112 and 122; where the unique, network coupling identifier is associated with the dedicated telephone line coupling the terminal to the network).

As per claim 11, Ensor et al. then point out:

associating a network user to the workstation (see column 3, lines 62-67; a user who has a particular subscriber terminal).

As per claim 12, Ensor et al. illustrate a method for providing security to a computer network by monitoring the network login or login attempt from a particular workstation, comprising:

associating a workstation to a physical location (see column 4, lines 19-25; figure 1, items 110 and 112; a terminal device for a home subscriber station connected by a telephone jack and line);

associating a network user to the workstation (see column 3, lines 62-67; a user who has a particular subscriber terminal);

monitoring a computer network to determine a network login or attempted login of the user (see column 4, lines 40-59; receiving from the network a unique, network coupling identifier for the particular terminal when the subscriber attempts to gain access to the network);

determining which workstation the login or attempted login is generated from (see column 5, lines 41-66; figure 1, items 110, 112,

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

and 126; figure 3, step 350; comparison of newly encrypted password stored in the database with the password retrieved from the terminal to determine a match or mismatch between the terminal and the dedicated telephone line); and

determining whether the user is authorized to access the network from the workstation of the login or attempted login (see column 5, lines 54-67; column 6, lines 1-6; figure 1, items 110, 112, 126, and 114; the transaction manager compares the newly encrypted password with the retrieved password where two nonidentical passwords indicate an unauthorized login attempt and two identical passwords indicate successful authentication where the subscriber is authorized to access the network from the terminal at the dedicated telephone line).

As per claim 13, Ensor et al. illustrate a network security system for a plurality of workstations coupled via a local area network, comprising:

electronic storage for associating the workstations to a user and a physical location (see column (see column 5, lines 3-21; figure 1, items 108, 112, and 110; encrypted passwords resulting from telephone numbers used to identify registered accounts for all terminals stored in the service bureau internal database for a subscriber);

one or more processors for receiving login information from the workstations login (see column 4, lines 51-63; figure 1, item 112 and 122; receiving the unique, network coupling identifier associated with the dedicated telephone line coupling the terminal to the network and; see column 5, lines 3-21; figure 1, item 126; the password stored in a predetermined location in the terminal memory stored during registration); and accessing electronic storage to determine whether the user or the workstation is authorized to login to the network from the physical location (see column 5, lines 54-67; column 6, lines 1-6; figure 1, items 110, 112, 126, and 114; the transaction manager compares the newly encrypted p.ssword with the retrieved password where two nonidentical passwords indicate an unauthorized login attempt and two identical passwords indicate successful authentication for the subscriber to access the network from the terminal at the dedicated telephone line).

As per claim 14, Ensor et al. further describe:

generating an alert based on the determination (see column 5, lines 60-66; figures 110, 112, and 126; sending an error message to the subscriber that the authentication has failed).

As per claim 17, Ensor et al. moreover point out:

that the alert comprises a termination signal (see column 5, lines 50-54; figure 3, step 330; instructing the network to terminate the modem connection to disconnect the subscriber from the network).

As per claim 22, Ensor et al. depict a network security system for a plurality of workstations coupled via a local area network (see column 3, lines 2-5; figure 1, items 100 and 110; a plurality of user terminals communicably coupled to a network), each workstation being associated with a specific user and coupled to one of a plurality of data ports of a patch panel, coupled to the a computer network (see column 3, lines 6-15; figure 1, items 110, 112 and 100; figure 2, items 202, 212, and 200; user terminals specific to the home or business of the subscriber coupled to the network via a uniquely identifiable network coupling such as a dedicated telephone line into a telephone network), comprising:

a workstation associated with a physical location and a user (see column 3, lines 6-15; figure 1, items 110, 112 and 100; figure 2, items 202, 212, and 200; user terminals specific to the home or business of the subscriber indicated by a dedicated telephone line);

a monitoring device for determining a network login or attempted login of the user (see column 4, lines 40-56; figure 1, items 110 and 108; the service bureau receiving from the network a unique, network coupling identifier for the particular terminal upon a modem call to the service bureau); and

a device for determining a physical location of the login or attempted login (see column 5, lines 3-53; figure 1, items 110, 112, and 114; the transaction manager determining the location and registration status of a particular terminal during the modem call from the telephone number);

where the system determines whether the user is authorized to access the network from the physical location of the login or attempted login (see column 5, lines 54-67; column 6, lines 1-6; figure 1, items 110, 112, 126, and 114; the transaction manager compares the newly encrypted password with the retrieved password where two nonidentical passwords indicate an unauthorized login attempt and two identical passwords indicate successful authentication for the subscriber to access the network at the dedicated telephone line).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/10507

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Claims 8-10 lack an inventive step under PCT Article 33(3) as being obvious over the Ensor et al., U.S. Patent No. 5,721,780 A as applied to claim 1 and further in view of Kondo et al., U.S. Patent No. 5,684,957 A.

As per claim 8, Ensor et al. specify workstation information including the jack or outlet information (see column 6, lines 26-42; figure 1, item 110, 108, and 112; updating the corresponding list of passwords by encrypting the network coupling identifier using a different encryption key after an initial password authentication for a selected terminal; see column 4, lines 51-63; figure 1, item 112 and 122; where the unique, network coupling identifier is associated with the dedicated telephone line coupling the terminal to the network). However, they do not describe the other details. Kondo et al. point out the date and time of each successful login (see column 17, lines 36-45; figure 14, items 1403; login times), domain address (see column 17, lines 36-45; figure 14, items 1401; names of virtual terminals; see column 17, lines 48-55; figure 15, item 1502; employed for login procedures), and information regarding which network resources were accessed (see column 19, lines 1-4; figure 19; accesses history information including names of files, access users, access process, and data and time of access). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Ensor et al. with the date and time of each successful login, domain address, and information regarding which network resources were accessed of Kondo et al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

As per claim 9, Ensor et al. teach the method of claim 1. However, they do not explicitly show an event log. Kondo et al. describe an event log (see column 17, lines 36-48; figure 14; a login records table). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Ensor et al. with the event log of Kondo c. al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

As per claim 10, Kondo et al. further elaborate:

that the event log comprises information regarding the physical location of the login or attempted login (see column 17, lines 36-41; figure 14, item 1402; names of login terminals; see column 12; lines 50-59; where the physical position of the named login terminal is assigned in a map database) and information regarding the user (see column 17, lines 36-41; figure 14, item 1400; names of login users). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Ensor et al. with the event log of Kondo et al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

Claims 15-16 lack an inventive step under PCT Article 33(3) as being obvious over the Ensor et al., U.S. Patent No. 5,721,780 A as applied to claim 14 and further in view of Day, U.S. Patent No. 6,311,274 B1.

As per claim 15, Ensor et al. describe the system of claim 14. However, they do not explicitly teach an email notification. Day illustrates that an alert includes an email notification (see column 2, lines 65-67 and column 3, lines 1-20; sending an e-mail message when an alert condition is met). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system of Ensor et al. with the email notification of Day to prevent an unauthorized party masquerading as a party authorized to send alerts and prevent unauthorized disclosure or modification of information contained in the alert (see column 1, lines 52-60).

As per claim 16, Day further describes:

that the alert comprises a pager notification (see column 5, lines 32-37; an alert action comprising sending a message to a pager). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system of Ensor et al. with the pager notification of Day to send the alert to a person as a recipient of the alert meant to receive such information (see column 5, lines 42-45).

Claims 18-20 lack an inventive step under PCT Article 33(3) as being obvious over the Ensor et al., U.S. Patent No. 5,721,780 A as applied to claim 14 and further in view of Kondo et al., U.S. Patent No. 5,684,957 A.

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

As per claim 18, Ensor et al. teach the system of claim 14. However, they do not explicitly show an event log. Kondo et al. describe an event log (see column 17, lines 36-48; figure 14; a login records table). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system of Ensor et al. with the event log of Kondo et al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

As per claim 19, Kondo et al. then discuss:

that the event log comprises a time of the access (see column 17, lines 36-45; figure 14, items 1403 and 1404; login times and logout times). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system of Ensor et al. with the event log of Kondo et al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

As per claim 20, Kondo et al. further elaborate:

that the event log comprises information regarding the physical location of the login or attempted login (see column 17, lines 36-41; figure 14, item 1402; names of login terminals; see column 12; lines 50-59; where the physical position of the named login terminal is assigned in a map database) and information regarding the user (see column 17, lines 36-41; figure 14, item 1400; names of login users). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the system of Ensor et al. with the event log of Kondo et al. to provide a network management system the capability of early detection of an unauthorized entry from outside and unauthorized use from inside by determining the status of accesses to a network device by leaving a record of accesses (see column 4, lines 60-67 and column 5, lines 1-4).

Claims 1-22 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry to prevent unlawful or unauthorized activities by an otherwise authorized network user (see description, page 2, ¶¶ [005]-[006]).